UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/275,722	03/24/1999	DAVID A. LEE	042390.P6526	1130

7590 03/10/2006

WILLIAM W SCHAAL
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/275,722	LEE, DAVID A.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 remain for examination.

Response to Arguments

2. In view of the appeal brief filed 12/28/05, PROSECUTION IS HEREBY REOPENED.

3. On page 15 of the appeal brief filed 12/28/05, Applicant alleges that claims 1, 3-11, and 13-27 were rejected under 35 USC 102(b) in view of the Lotspiech reference. That is incorrect; the status of those claims at that time was that they had been rejected under 35 USC 102(e).

4. On pages 10, 13, and 14 of the appeal brief filed 12/28/05, Applicant alleges that claims 1-18 were rejected under 35 USC 101 as having no utility. This is incorrect; the Office Action of 8/10/05 stated rather clearly that the claims were rejected as being non-statutory subject matter (see page 3 of that Action). Applicant's argument – originally presented on pages 10 and 11 from the amendment filed 12/01/03 – is thus moot, as the utility of the claims was not in dispute in the previous Action.

5. Applicant's arguments filed in the appeal brief filed 12/28/05 have been fully considered but with respect to claims 11-27 they are not persuasive.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., producing a secret device key from at least two selected rows in a matrix, as argued on page 16 of the appeal brief) is not recited in independent claims 11, 19, 20 or

23, nor in the claims dependent therefrom. Claim 11 recites producing a secret device key from at least two selected columns in a matrix, not rows; this is a significant distinction as noted below (see "Allowable Subject Matter"). Claim 20 recites generating a key vector by selecting individual keys, with no constraints as to the particular rows and columns involved. Claims 19 and 23 lack any recitation of using a key matrix to create a shared secret key. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant's arguments with respect to claims 11-18 have been considered but are moot in view of the new ground(s) of rejection.

6. Applicant's arguments, see pages 15-18 of the appeal brief filed 12/28/05, with respect to rejection of claims 1-10 and the objection of claim 19 have been fully considered and are persuasive. The rejection of claims 1-10 over Lotspiech (and per claim 2, in view of Luther), as well as the objection of claim 19, has been withdrawn.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 23-27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 23 recites a memory for storing a key matrix

with a plurality of rows and columns, and logic to generate a key selection vector for each digital device registered with the certification authority. The two limitations do not appear to be interrelated in any way: the claimed memory does not store the logic, nor does the claimed logic recite any use for the memory or its contents. Additionally, the limitations by themselves are insufficient to perform the functions of a certification authority as recited in the preamble, even when considered in its broadest reasonable sense. Thus, the body of the claim appears to be incomplete, or the preamble appears to be inaccurate. Claims 24-27 are rejected by virtue of their dependency on claim 23.

Claim Rejections - 35 USC § 101

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claims 1 and 11 recite a series of abstract steps in an algorithm that ultimately produces a shared secret key; however, it is clear from the disclosure that the producing step at most only relates to creating a piece of data (the shared secret key) per se, without communicating said shared secret key or disclosing it in any way such that it could be operated by any other entity. The instant specification even teaches away from doing so, as the novelty of the invention lies in the ability for devices that wish to communicate with each other to independently generate the secret key through the use of intermediary information (Figure 3 and page 14, line 17 – page 15, line 23 of the instant specification for example). Thus, the end

result of the claimed process is a thought or result of a computation of a processor, which is not a tangible result as dictated by statute and current Office practice. The dependent claims do not rectify the issue, and thus stand rejected for similar reasons.

11. Claims 23, 24, and 27 are rejected under 35 U.S.C. 101 because the claimed limitations do not fully realize a properly functioning certification authority. The claims lack essential steps that would relate the recited elements. Although the disclosed certification authority has utility, the limitations recited in these claims are at best preliminary steps that do not realize any usefulness in and of themselves.

Claim Rejections - 35 USC § 102

12. Claims 19-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Lotspiech et al. (U.S. Patent 6,118,873).

Referring to Claim 19:

Lotspiech discloses a machine readable medium having embodied thereon a computer program for processing by a first digital platform including memory containing the computer program comprising: an authentication function to recover an incoming key selection vector and to compute a shared secret key based on a set of secret device keys stored in the first digital platform and the contents of the incoming key selection vector (col. 5, line 42 – col. 6, line 42); a transfer function to output at least a key selection vector assigned to the first digital platform (col. 6, lines 30-40); a hash function to perform a hash operation on at least the shared secret key to produce a

resultant hash value (col. 6, lines 30-40); and a comparison function to compare the resultant hash value with an incoming check hash value received subsequent to the transmission of the key selection vector (col. 6, lines 30-40; col. 6, lines 20-30).

Referring to Claim 20:

Lotspiech discloses a network comprising: a first digital platform; and a certification authority in communication with the first digital platform (Fig 1; col. 5, lines 1-20), the certification authority having access to a key matrix featuring matrix keys arranged in accordance with at least a first dimension and a second dimension (col. 5, lines 10-41), generating a first key selection vector and providing a first set of secret device keys produced from selected matrix keys of the key matrix (col. 5, lines 42-54).

Referring to Claim 21:

Lotspiech discloses the limitations of Claim 20 above. Lotspiech further discloses a second digital platform in communication with the certification authority and the first digital platform (col. 6, lines 55-68; col. 8, lines 30-40), the second digital platform being uniquely assigned a second key selection vector indicating at least two grids of the key matrix (col. 6, line 60-col. 7, line 10) and a second set of secret device keys produced from matrix keys situated in at least two grids of the key matrix (col. 7, lines 10-25).

Referring to Claim 22:

Lotspiech discloses the limitations of Claim 21 above. Lotspiech further discloses the first and second digital platforms to exchange the first and second key selection vectors in order for each digital platform to produce a shared secret key to ensure that communications between the first and second digital platforms are secure (col. 8, lines 30-45; col. 9, lines 34-49).

Referring to Claim 23:

Lotspiech discloses a certification authority comprising: a memory to store a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2 (Figure 3; and col. 5, lines 10-41); and a logic to generate a key selection vector for each digital platform registered with the certification authority (col. 5, lines 42-54).

For the record, Examiner wishes to note that Lotspiech's use of the arbitrary designation "N" corresponds to Applicant's use of "M", and Lotspiech's use of the arbitrary designation "M" corresponds to Applicant's use of "N".

Referring to Claim 24:

Lotspiech discloses the limitations of Claim 23 above. Lotspiech further discloses the logic includes a processing unit (col. 4, lines 5-20).

Referring to Claim 25:

Lotspiech discloses the limitations of Claim 24 above. Lotspiech further discloses the processing unit produces a first set of secret device keys by performing arithmetic operations on matrix keys along selected columns of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform (col. 5, lines 42-54).

Referring to Claim 26:

Lotspiech discloses the limitations of Claim 24 above. Lotspiech further discloses the matrix keys along the processing unit performs arithmetic operations on matrix keys along selected rows of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform (col. 5, line 42 – col. 6, line 41).

Referring to Claim 27:

Lotspiech discloses the limitations of Claim 23 above. Given that it is undesirable for another entity to learn even one key in the matrix (e.g. col. 6, lines 42-51), it is thus inherent to the security of the disclosed system that the matrix keys must only be known by the certification [licensing] agent (col. 5, lines 15-20).

Claim Rejections - 35 USC § 103

13. Claims 11 and 13-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech (U.S. Patent 6,118,873).

Referring to Claim 11:

Lotspiech discloses a method comprising providing a key matrix having N rows and M columns, where N>2 and M>2 (Figure 3; col. 5, lines 20-41); for each row of the matrix, performing arithmetic operations utilizing matrix keys of at least two selected columns to produce a secret device key which is a part of a first set of secret device keys (col. 5, lines 42-54), and producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys (col. 5, line 55 – col. 6, line 12).

For the record, Examiner wishes to note that Lotspiech's use of the arbitrary designation "N" corresponds to Applicant's use of "M", and Lotspiech's use of the arbitrary designation "M" corresponds to Applicant's use of "N".

With respect to the limitation regarding "for each row...utilizing matrix keys of at least two columns", Lotspiech discloses wherein for at least one row the system uses keys from at least two columns ($S_{1,3}$ and $S_{1,4}$ in Figure 3), although it is not mandated that this condition be satisfied. Nevertheless, in the preferred embodiment of Lotspiech wherein the matrix has 32 rows and 128 columns (col. 7, lines 37-39) for example, it is not only possible but highly probable (in excess of 90% likely) that following the process disclosed in col. 5, lines 42-54 will result in a scenario wherein each row of the matrix

will have keys from at least two columns selected. Accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to explicitly stipulate an embodiment of Lotspiech wherein for every row device keys from at least two columns are selected. The motivation for doing so would be to eliminate trivial cases (such as selecting all the keys from exactly one row) which could negatively affect the randomness of the key distribution, and by extension weaken the security of the overall system.

Referring to Claim 13:

Lotspiech discloses or suggests the limitations as discussed in Claim 11 above. Lotspiech further discloses prior to performing the arithmetic operations, the method comprises: generating a key selection vector identifying the at least two selected columns of the key matrix from which to produce the first set of secret device keys (col. 5, lines 42-54).

Referring to Claim 14:

Lotspiech discloses or suggests the limitations as discussed in Claim 11 above. Lotspiech further discloses the key selection vector is uniquely assigned to a first digital platform (col. 5, lines 52-54).

Referring to Claim 15:

Lotspiech discloses or suggests the limitations as discussed in Claim 14 above. Lotspiech further discloses wherein prior to producing the shared secret key, the method comprises: receiving a key selection vector from a second digital platform in communication with the first digital platform (col. 5, lines 40-50); and analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys (col. 5, lines 10-30, 40-65).

Referring to Claim 17:

Lotspiech discloses or suggests the limitations as discussed in Claim 11 above. Lotspiech further discloses producing of the shared secret key comprises: analyzing contents of an incoming key selection vector (col. 5, line 55 – col. 6, line 12); and performing arithmetic operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector (Ibid).

Referring to Claim 18:

Lotspiech discloses or suggests the limitations as discussed in Claim 17 above. Lotspiech further discloses the producing of the shared secret key further comprises: performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector (col. 6, lines 34-40).

14. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech, and further in view of Luther (U.S. Patent 5,533,127).

Referring to Claim 12:

Lotspiech discloses or suggests the limitations as discussed in Claim 11 above.

Lotspiech does not explicitly disclose "the arithmetic operations include modular addition." However, Luther discloses this limitation (col. 7, lines 35-50; Fig .9).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Lotspiech such that arithmetic operation is modular addition. One of ordinary skill in the art would have been motivated to do this because it would provide a method for generating a common key (Lotspiech: col. 6, lines 35-42).

Allowable Subject Matter

15. Claims 1-10 would be allowable if rewritten to overcome the rejection under 35 USC 101 above.

16. The following is a statement of reasons for the indication of allowable subject matter: Further examination of the prior art cited in the previous rejection reveals that Lotspiech explicitly teaches away from the invention of claim 1, by stipulating that for each column in the matrix, no more than one row can be selected for the set of secret device keys (col. 5, lines 47-52).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
3/2/06

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100